

LISTING OF CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) An electronic device in a local area network, comprising:
a network interface that communicates with a connection point of the local area network
(LAN), and that receives a polling signal from a security system in the local area network via the
connection point; and

a control that causes the network interface to communicate a response to the security
system via the connection point in response to receipt of the polling signal, and said control
verifies that said electronic device is installed in an authorized network and generates an alarm if
said electronic device is not present and, said control causes the network interface to
communicate the response to the security system as an encrypted message using an encryption
code that is unique to the electronic device;

wherinc said message includes an address and an identifier associated with the electronic
device and said control verifies that said electronic device is installed in an authorized network
based upon said address and said identifier; and

wherein said user interface is configured to allow a user to arm and disarm [[a]] building
intrusion detection features separately from security features of said LAN.

2. (Original) The electronic device of claim 1, wherein:

the network interface communicates with at least one other electronic device in the local
area network via the connection point to transfer entertainment content.

3. (Original) The electronic device of claim 1, wherein:

the network interface communicates, via the connection point, with a remote server that
provides services for the electronic device.

4. (Original) The electronic device of claim 3, wherein:

the services include at least one of downloading software to the electronic device, performing remote programming of the electronic device, and uploading diagnostic data from the electronic device.

5. (Original) The electronic device of claim 1, wherein:
the connection point comprises at least one of a hub and a gateway.

6. (Original) The electronic device of claim 1, wherein:
the network interface receives software from the security system via the connection point for configuring the electronic device as a sensor of the security system.

7. (Original) The electronic device of claim 1, wherein:
the security system sets an alarm if it does not receive the response from the network interface after sending the polling signal to the network interface.

8. (Canceled)

9. (Original) The electronic device of claim 1, wherein:
the control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique for a specified group of electronic devices.

10. (Currently Amended) A security system, comprising:
a network interface that communicates with a connection point of a local area network (LAN); and
a control that causes the network interface to transmit a polling signal to an electronic device in the local area network via the connection point, said control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device;

wherein said message includes an address and an identifier associated with the electronic device and said control verifies that said electronic device is installed in an authorized network based upon said address and said identifier;

wherein the control sets an alarm if a response to the polling signal is not received from the electronic device; and, to verifies that said electronic device is installed in an authorized network;

wherein said network interface is configured to allow a user to arm and disarm [[a]] building intrusion detection features separately from security features of said LAN.

11. (Original) The security system of claim 10, wherein:

the electronic device communicates with at least one other electronic device in the local area network via the connection point to transfer entertainment content.

12. (Original) The security system of claim 10, wherein:

the network interface communicates, via the connection point, with a remote server that provides services for the security system.

13. (Original) The security system of claim 12, wherein:

when the alarm is set, the network interface communicates a message to the remote server indicating that the alarm has been set.

14. (Original) The security system of claim 13, wherein:

the message comprises an identifier of the electronic device.

15. (Original) The security system of claim 13, wherein:

the message comprises at least a portion of an Internet Protocol address associated with the electronic device.

16. (Original) The security system of claim 10, wherein:

the connection point comprises at least one of a hub and a gateway.

17. (Original) The security system of claim 10, wherein:
the network interface transmits software to the electronic device via the connection point
to configure the electronic device as a sensor of the security system.

18. (Original) The security system of claim 10, further comprising:
means for monitoring at least one sensor for detecting intrusion in a building.

19. (Cancelled)

20. (Original) The security system of claim 10, wherein:
the response to the polling signal is provided as an encrypted message using an
encryption code that is unique for a specified group of electronic devices.

21. (Canceled)

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Canceled)

26. (Canceled)

27. (Canceled)

28. (Currently Amended) A security system server, comprising:
a network interface that receives a message that includes an address and an identifier
associated with an electronic device;

wherein the electronic device is provided in a local area network LAN; and
a control means for determining whether the address is consistent with the identifier, said
control means verifies that said electronic device is installed in an authorized network based
upon said address and said identifier and generates an alarm if said electronic device is not
present, and said control causes the network interface to communicate the response to the
security system as an encrypted message using an encryption code that is unique to the electronic
device;

wherein said message includes an address and an identifier associated with the electronic
device;

and said network interface is configured to allow a user to arm and disarm [[a]] building
intrusion detection features separately from security features of said LAN.

29. (Original) The security system server of claim 28, wherein:
the message is received from the electronic device.

30. (Original) The security system server of claim 28, wherein:
the message is received from a server that provides services for the electronic device.

31. (Original) The security system server of claim 28, wherein:
the address comprises at least a portion of an Internet Protocol address.

32. (Original) The security system server of claim 28, wherein:
the identifier comprises a serial number.

33. (Original) The security system server of claim 28, wherein:
the message is received as an encrypted message using an encryption code that is unique
to the electronic device.

34. (Original) The security system server of claim 28, wherein:

the message is received as an encrypted message using an encryption code that is unique for a specified group of electronic devices.

35. (Previously Presented) The electronic device of claim 1, wherein said control is configured to not allow spoofing of said electronic device.

36. (Previously Presented) The security system of claim 10, wherein said control is configured to not allow spoofing of said electronic device.

37. (Canceled)

38. (Previously Presented) The security system server of claim 28, wherein said control is configured to not allow spoofing of said electronic device.